ORANGE TRANSPARENCY REPORT
ON FREEDOM OF EXPRESSION AND PROTECTING PRIVACY

2020 data

Orange is one of the world's leading telecommunications carriers with a turnover of €42.3 billion in 2020 and 142,000 employees as at December 31, 2020, of whom 82,000 are in France. The Group has a total customer base of 259 million customers worldwide at December 31, 2020, including 214 million mobile customers and 22 million fixed broadband customers. The Group is present in 26 countries. Orange is also a leading provider of global IT and telecommunication services to multinational companies, under the brand Orange Business Services.

Contents

1. The Orange Group's commitment to freedom of expression and privacy

1.1. Orange strives to act in accordance with the human rights defined by the United Nations in its Universal Declaration of Human Rights[1.]

As a telecommunications carrier, Orange strives to ensure that human rights are respected at all times when using Information and Communication Technologies (ICT), and more specifically for:

- article 12: “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks. ”
- Article 19: “Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers. ”
- Article 29: “1. Everyone has duties to the community in which alone the free and full development of his personality is possible. 2. In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society. 3. These rights and freedoms may in no case be exercised contrary to the purposes and principles of the United Nations. ”

1.2. Orange, committed as a member of the Global Network Initiative (GNI)

The Orange Group’s commitment to promote freedom of expression and privacy in its activities as a telecommunications carrier is guided by its membership of the Global Network Initiative (GNI).

In March 2017, Orange and a number of carriers and device manufacturers from the sector-based group Telecom Industry Dialogue (TID) joined the GNI (https://globalnetworkinitiative.org/), of which Orange is currently a member of the Board of Directors. This multi-stakeholder platform, which includes internet carriers, telecommunications carriers, device manufacturers, NGOs, academics and socially responsible investors, focuses on issues of freedom of expression and protection of privacy in response to government requests. The GNI’s Guiding Principles[2] constitute a reference for the development and implementation, within the Orange Group, of policies and processes relating to freedom of expression and the right to privacy in its activities as a telecommunications carrier. Every year, Orange issues a report on the actions put in place to fulfill these principles. Since 2019 (for 2018 data), this self-assessment report has been further reinforced and subject to an assurance report by an independent third-party organization appointed by the GNI. In accordance with GNI governance, this specific audit on the implementation of its Principles relating to freedom of expression and privacy is repeated every two to three years; it specifically supplements the Orange Group’s non-financial statement, which is itself reviewed annually by an independent third-party and subject to a public assurance report in its management report.

1.3. Orange’s commitment to the right to privacy when collecting and hosting the personal data of its employees, customers and business partners

Orange is committed around four principles:

- safeguarding customer personal data through reliable processing and secure storage,
- customer control over personal data,
- transparent processing of customer and user data at all stages of the relationship, via dedicated

[1] https://www.un.org/en/universal-declaration-human-rights/index.html

[2] GNI Principles

information and personal data processing policies accessible through Orange applications and sites,
- support for all customers and users to help them to protect their privacy and better manage their personal data, e.g. via information campaigns.

Orange also ensures that it conveys these commitments to its subcontractors and business partners.

The Orange Group's internal policy in terms of personal data protection is based on the following commitments:

- Data Protection from Design ("Privacy By Design") and respect for the main principles of personal data protection: Orange undertakes to protect Personal Data through a proactive, preventive and risk-based approach, in particular from the design of the products and services of the Orange Group.
- An organization and procedures for evaluating processing in terms of compliance and ensuring the exercise of the rights of individuals (lawfulness of processing, transparency and loyalty, legitimacy and clarification of the purposes of processing, limitation of the duration of conservation, ...)
- Security: Orange undertakes to implement the required technical and organizational measures to safeguard confidentiality and protect Personal Data against any accidental, unauthorized or unlawful access, use, modification, disclosure, loss, destruction or damage, pursuant to the Group Security Policy.
- Accountability: Orange undertakes to demonstrate compliance with the applicable data protection Law(s) at all times. For this purpose, the Group and Orange entities will implement and document the measures and means to demonstrate compliance and efficacy of the measures taken at the time.
- A governance with the contribution of the networks of data protection officers.
- Appropriate actions and documentation to monitor all of its processing activities as well as, for example, employee awareness.

1.4. Orange's commitment to responsible and non-discriminatory use of its services, particularly when using artificial intelligence

In 2019, Orange reiterated its commitment by establishing a purpose to be included in its Bylaws guaranteeing that, in all areas of business, digital is designed, made available and used in a more human, inclusive and sustainable manner. The Engage 2025 strategic plan embodies this purpose, itself built on the idea that economic performance is achieved through social and environmental excellence.

The Group's commitment is reflected by a selection of 6 Sustainable Development Goals (SDG) established by member states of the United Nations, where the Orange Executive Committee believes that the Group has or should make a substantial positive contribution. The implementation of Orange commitments and more generally its business conduct is based on the principles for action covered by SDG 16 (peace, justice and strong institutions) and SDG 17 (partnerships for the goals).

Orange's commitment to contribute to SDG 16 relates to data protection and specifically personal data, transparency and openness, whilst promoting ethical behavior among all stakeholders. Orange has also established an anti-corruption system at Group level. The success of all these actions relies on close cooperation with other players in the ecosystem.

Personal data protection benefits from the general data security framework established by Orange, which covers both corporate information and personal data. It is one of the major areas which Orange intends to develop to support its Engage 2025 strategic plan. It is governed by a Security Policy, which aims to continually improve security through risk assessment and management (particularly cyber risks).

2. Governance within Orange to enforce its commitments in terms of freedom of expression and privacy in its area of influence

2.1. Group risk management framework

Group risks are presented to the Group risk committee at least annually. This Committee is supervised by the Chairman and CEO, and chaired by the Deputy CEO, the Executive Director for Finance, Performance and Development. It comprises members of the Executive Committee, and its role is to review risks and suggest decisions to control them.

The overall risk management assessment is also presented to directors during a joint meeting of the board of directors' committees, when major risks are discussed in the presence of relevant directors. Orange is ISO 9001 certified for its Group Risk Management approach.

Risks in terms of the violation of human rights and fundamental freedoms and the disclosure or modification of personal data are encompassed in the Group risk control framework: they are described in the Group risk framework linked to the Duty of Due Diligence with its consequences, causes, risk control systems and their level of implementation; they are then assessed in view of all these elements at Group and local level. The control systems in place address the causes of risks to limit the consequences on probability and/or impact.

2.2. Governance in terms of personal data protection

Orange and its entities set up governance for the protection of personal data according to their internal organization and in accordance with local legal requirements.

The European General Data Protection Regulation (GDPR) is of particular importance to Orange, even if Orange takes into account all the regulations that would apply to it worldwide.
The General Data Protection Regulation entered into force on May 25, 2018. This general text is applicable to public and private entities, and standardizes the management of personal data protection across Europe. The GDPR notably includes the principles of unambiguous consent which explicitly applies to personal data processing, the definition of a pseudonymization process whose use is encouraged, strengthening the duty to provide information to consumers, and the introduction of the "right to be forgotten."
To provide expert support in this area to the group's entities and its various businesses, and meet protection standards, Orange has appointed Data Protection Officers in the entities. At Group level, the Personal Data Protection Officer reports to the Legal Director.

The protection framework applies to relations within the group and with all group service providers and partners. It aims to prioritize focal points regarding the effectiveness of individual rights and the required transparency (negotiating partnerships or services, or creating customer or service user journeys). Risks linked to personal data protection violations are presented to the Group risk committee on an annual basis.

2.3. Supervision of freedom of expression and the right to privacy by the Group's Corporate Social Responsibility department

The Orange Group's Corporate Social Responsibility (CSR) department, which reports to the Executive Director of Social Responsibility, supervises compliance with Orange Group commitments to freedom of expression and the right to privacy and their promotion. It regularly reports directly to the Group executive committee and via the Ethics and Sustainable Performance Committee, and to the Orange Board of Directors via the Social and Environmental Responsibility Governance Committee (CGRSE). The Orange Executive Committee and its Board of Directors are thus made aware and take a position regarding major human rights decisions.
In addition, to meet its international obligations, Orange publishes a Declaration on Modern Slavery and Human Trafficking (MSA), signed annually by the President of Orange.
Group CSR collaborates with the Group Risk Management, Control & Audit department. It benefits from the work presented by other divisions to the Orange risk committee on non-financial risks, and relies on the Group's risk coverage and assessment methodology. It also uses this methodology to deploy its risk coverage process within entities, and takes part in division internal control reviews.

2.4. Inclusion of human rights in the Orange Group's Duty of Vigilance

The French law on the Duty of Vigilance has provided all Group entities with a regulatory framework reinforcing its due diligence, steering and deployment of its action plans relating to human rights and fundamental freedoms. Orange publishes its vigilance plan[3] and the implementation report[4] every year. Orange also publishes a Modern Slavery and Human Trafficking Statement.

The risks to human rights identified by Orange in its vigilance plan include the following elements:

- human slavery and trafficking,
- indecent work conditions (including at suppliers and subcontractors),
- abuse of children's rights to education and harmonious development,
- abuse of the freedom to be a union member and collective bargaining for work conditions,
- discrimination,
- abuse of the freedom of expression (in civil society),
- invasion of privacy.

This report specifically covers the final 2 risks identified at Group level.

2.5. Application of GNI principles

Like all other GNI members, Orange's progress in implementing GNI principles is assessed regularly and independently. The purpose of the assessment is to allow the GNI board of directors to determine whether each member company is making its best efforts, in good faith, to implement its principles as part of a continuous improvement approach. The independent assessment includes an examination of the company's processes (systems, policies and procedures) and an examination of specific case studies. It concluded that the implementation of GNI principles is a priority for the Group, that the principles are integrated within Orange policies, and that Orange endeavors, in good faith, to implement GNI principles as part of a continuous improvement approach. These results were published by GNI in April 2020 in its "GNI Public Assessment Report[5] ".

3. The Orange Group's assessment of the risks of violating freedom of expression and privacy in its area of influence.

3.1. Risk assessment linked to personal data protection

"Personal data" refers to any information about an identified individual or individual who can be identified, directly or indirectly, notably by reference to an identifier such as an ID number, location data, online login, or one or several elements specific to their physical, physiological, genetic, mental, economic, cultural or social identity.

The Orange risk assessment relates to loss, disclosure or unauthorized communication to third parties, or inappropriate modification of the personal data of Orange customers, its employees or the general public, whether this data is stored on its infrastructure or carried by its networks.

This risk assessment by each Group entity is based on reviews and/or internal surveys to verify compliance with laws and regulations over time. Each Orange group entity creates a map to identify operations in personal data categories within the entity, and establishes a Processing Activities Record[6] in accordance with applicable data protection laws and its

[3] Orange 2021 Vigilance plan

[4] Orange 2020 Viglance plan report

[5] GNI Principles Implementation Report

[6] refers to any operation or all operations using Personal Data or sets of Personal Data, whether automated or not, such as the collection, recording, organization, structuring, storage, adaptation or modification, extraction, consultation, use, disclosure by transmission, distribution or any other form of provision, combination, deletion or

internal organization. This map identifies Special Personal Data Categories (often known as "sensitive data"), i.e. Personal Data which, by its nature, is particularly sensitive with regards to human rights and fundamental freedoms, and is subject to special protection; its Processing might pose significant risks for the Data Subjects (e.g. data which reveals ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, data about health or sex life, etc.). The Processing of Special Personal Data Categories is only authorized in specific cases outlined in the applicable data protection law.

Other than the processing activities record, this risk assessment also includes an incident management and personal data infringement notification section.

3.2. Mapping risks of violations of human rights and fundamental freedoms

Each year, Orange has a risk assessment carried out relating to human rights and fundamental freedoms by a specialized organization, Verisk Maplecroft, for every country where it operates. This organization considers the level of risk for each country for different human rights aspects. Orange uses this information to adapt its own "Human Rights and Fundamental Freedoms" risk map each year. Adapting this assessment solely to the criteria of interfering with freedom of expression and invasion of privacy leads Orange to determine criteria corresponding to its risk assessment in terms of human rights due to its activities and geographic locations, based on 10 risk criticality indexes and allowing an aggregated rating, country by country. These aspects cover State robustness in terms of the degree of corruption, democratic governance, the power of the judiciary in terms of reach and effectiveness, as well as respect for the rights of minorities.

They are supplemented by more specific aspects as an essential infrastructure operator, which are digital inclusion, freedom of expression and opinion, and due to the large number of government subpoenas, interceptions of communications or telephone and internet network shutdowns, government stability and civil unrest aspects are also included for the first time in 2020. These network shutdowns are perceived as an obstacle to holding democratic elections, as they restrict freedom of expression, access to information and freedom of the press. Beyond these restrictions, a network shutdown during elections undermines public confidence in the electoral process.

In its 2020 impact study on human rights relating to freedom of expression and privacy, based on the scores assigned by the consultancy firm Verisk Maplecroft as part of the analysis described above for the entire Orange perimeter as a carrier, Orange believes that at the end of 2020 there are 3 geographic locations where the Group operates which require closer attention with regards to respect for human rights and fundamental freedoms. These are Mali, the Democratic Republic of the Congo and the Central African Republic. These 3 countries represent 1260 people directly employed by Orange to serve over 23.5 million customers. Still based on the criteria defined by the risk analysis, 6 additional countries are determined by Orange as requiring special attention in terms of human rights and fundamental freedoms. These are Guinea, Guinea Bissau, Cameroon, Egypt, Burkina Faso and Madagascar. These countries represent 24,553 people directly employed by Orange to serve over 56.3 million customers.

3.3. Special focus during election campaigns to ensure business continuity

The Group believes that election periods require special attention to prevent risks relating to freedom of expression and privacy.

In the Africa & Middle East region, the Orange Group has established pre-crisis units, which are activated and coordinated jointly by the region's business continuity and security departments before election periods until the results are announced. With the involvement of the subsidiaries in question and support from the Group security department, they verify that procedures have been put in place to allow our staff to safely continue their essential duties.

---

destruction.

4. Measures to mitigate the risks of violating freedom of expression and privacy implemented by the Orange Group.

4.1. Measures put in place to ensure personal data protection

To ensure proper application of the Personal data protection charter supplemented by the internal policy, the Orange Group has a general security policy to protect data, as well as a network of dedicated contacts to ensure all entities comply with Group requirements in terms of personal data protection[7]. When they handle matters relating to Personal Data and/or privacy, Orange Group entities cooperate to safeguard their image, as well as the Orange brand's reputation.

4.2. Preventive dialog with the authorities to determine the risk of denial of the freedom of expression and privacy

Orange regularly enters into dialog with local stakeholders to better understand the needs of local communities and authorities. In 2020, country dialog covering the notions of freedom of expression and data protection were held in Sierra Leone, Poland and Tunisia, and in Madagascar, Slovakia, Jordan and France in 2021.

Orange also carries out socio-economic footprint studies in each country, indicating its direct, indirect and induced contribution through social responsibility actions in terms of creating value and jobs. The direct and obvious consequence of any service shutdown by the authorities is a loss of wealth creation for the country.

4.3. 2020 contribution via the Global Network Initiative (GNI).

The GNI transparently represents the interests of non-governmental organizations, and it is listed on the transparency register with the European Commission, the Council of Europe and its human rights commission, the United Nations through special mandates, the counter-terrorism committee, the OHCHR (particularly for the B-Tech project), UNESCO and the GSMA. Through a single channel, it expresses the interests defended by its members in line with its Principles, entering into dialog with governments and international institutions to make recommendations on local policies and legislative changes, in order to enforce freedom of expression and privacy worldwide.

Initiatives in which the GNI is formally involved

Christchurch Call Advisory Network

Freedom Online Coalition Advisory Network

Internet & Jurisdiction Policy Network

OECD Project on Voluntary Transparency Reporting for Terrorist and Violent Extremist Content

Global Internet Forum to Counter Terrorism (GIFCT)

In 2020, Orange contributed to these recommendations on the following themes:

- there are an increasing number of government requests for network shutdowns, GNI reiterates the formal process which authorities must follow and the legitimate right of carriers to ensure this formal process is followed;
- the regulation of internet content, and the role of platforms regarding their conciliatory role to maintain user trust; as per the principle of net neutrality, the carrier can only restrict access to content following a legal ruling;
- the issues derived from the increased number of access points to the network due to new services created by the development of 5G networks, which are entrances requiring data

[7] See the Orange Universal Registration Document, page 294

protection to ensure privacy, and

- the impact of artificial intelligence on human rights, as the processing of data by algorithms could lead to discrimination.

4.4. Legal watch

To be able to confidently exercise its authority to object to any unjustified request, Orange monitors the latest legal provisions allowing the authorities to require network shutdowns or the interception of communications, particularly before elections are held. GNI members continually update a shared database, and the GNI regularly publishes changes to the legal framework in countries where its members operate[8]

France: Regulations on the interception of communications and the obligation of telecommunications carriers to disclose customer data

The commonly recognized principle of disclosure remains based on the fact that all requests must be made officially.

They can take a number of forms:
1. Requests from the judicial system: they come from legal decisions, as a result of the application of various laws:
a. Code of Criminal Procedure
b. The Postal and Electronic Communications Code

2. Requests from a government body under the supervision of a judge or from an independent administrative body (CNCTR or CNIL), in accordance with the Internal Security Code.

4.5. Interpellation of the civil society

Despite seeking a constant dialog with the authorities, Orange is sometimes required, in collaboration with the Global Network Initiative (GNI) and non-government organizations, to raise public awareness on discriminatory actions or actions which violate human rights and fundamental freedoms.

These alerts are analyzed internally and approved by operational entities.

In some situations, it gets the government to backtrack regarding unlawful requests.

[8] GNI Country legal frameworks resources

Example of how a repeated and reiterated request from the authorities in Guinea was handled by Orange in 2019:

Like other carriers in Guinea, Orange received a request from the national telecommunications regulator to access a platform for roaming calls, which contained a significant amount of customer data.

Orange sought to obtain a joint response by carriers to underline the unlawfulness of this request, the invasion of privacy as stipulated in article 116 of the Guinean law on ICT # 18 dated August 13, 2015, and the infringement of article 12 of the Universal Declaration of Human Rights.

In response, the authorities increased the carriers' tax bill, applying penalties for a failure to comply with the request.

The Orange Group resorted to a public appeal to expose these actions, and launched an international alert with NGOs. These actions led to the request being withdrawn and the government's public reiteration of its support of the principles of personal data protection, respect of fundamental freedoms and international agreements.

In this case, Orange demonstrated that the situation was handled by defending GNI principles relating to privacy and the safety of its employees.

4.6. Responsible use of data and artificial intelligence

In its Engage 2025 strategic plan, Orange identified aspects of artificial intelligence (automatic learning, deep learning, etc.) as a tool for its performance, boosting digital transformation.

To ensure the effective implementation of its commitment for responsible use of data and artificial intelligence, Orange created its Data and AI Ethical Council[9] in March 2021, with 11 members recognized in the field. Chaired by the Orange Chairman and Chief Executive Officer, the role of this independent advisory body is to support the company's implementation of ethical principles governing the use of data and Artificial Intelligence technologies. Orange thus supports the approach described in the document from the High Level Expert Group of the European Commission "Ethics Guidelines for Trustworthy Artificial Intelligence" and draws inspiration from its major principles:

- the purpose of artificial intelligence is to make a positive contribution to societal and environmental issues;
- artificial intelligence-based solutions must always respect human needs and be supervised by them;
- they must respect diversity and address risks of bias or discrimination;
- data used in artificial intelligence algorithms must respect privacy and be governed closely;
- the robustness and safety of AI-based solutions must correspond to the specific issues of each use;
- the functioning of AI-based solutions must be explained transparently and clearly, and the chain of responsibility must be clear.

As part of the discussion on inclusive and responsible artificial intelligence, the Orange Group is a member of the ImpactAI board of directors, a group of figures in artificial intelligence, with two shared objectives: addressing the ethical and societal issues of AI, and supporting innovative and positive projects worldwide.

Orange ensures that the entire data value chain is responsible and that potential discriminatory bias is identified and controlled. An audit conducted by Bureau Veritas assessed Orange in view of the GEEIS-AI reference framework for its actions in terms of the design, development and use of inclusive artificial intelligence. By obtaining this certification in December 2020, Orange demonstrates its commitment to digital equality. It follows on

[9] Data and AI Ethical Council

from the signing of the International Charter for Inclusive AI which was launched jointly by the Arborus endowment fund and Orange on April 21, 2020 and signed by around fifty organizations and companies, including Orange. It confirms that Orange uses AI from design through to application to promote diversity, ensuring that the entire data value chain is responsible and that potential discriminatory bias is identified and controlled.

5. Scope of violations of freedom of expression or privacy in Orange business in 2020

5.1. Nature of violations

Like all telecommunications operators, Orange must comply with government orders as defined by national security regulations and the law. This is a universal obligation which is laid out in each country's laws and regulations, as well as in licenses for telecommunications operations worldwide.

The reason for a government request to interrupt a service is increasingly linked to the election process (near an election, during the election itself, even during the count process). Orange might receive several different and simultaneous requests from the authorities: request to reduce internet speeds, limit access to certain social networks, shut down different categories of telecommunications services.

5.2. Orange's commitment to transparency

In terms of personal data protection, Orange undertakes to inform data subjects in a transparent fashion. Advance information must be given before any Processing and it must remain available, particularly when Processing is based on consent. The information made available to the data subject must be understandable, easy to access and formulated in clear and simple terms. Data subjects are also informed of their rights, including their right to file a complaint with the national supervisory bodies responsible for enforcing personal data regulations.

Orange has committed to regularly publishing information on government requests, to the extent permitted by local legislation. This approach guarantees transparency in terms of monitoring human rights-related government requests, particularly those related to the ICT sector.

For the sixth year running, Orange is publishing a report on government requests related to freedom of expression and protection of privacy.

5.3. Application of GNI principles

As a member of the GNI board of directors, Orange endeavors to respect the general principles, such as:

- respect and work to protect the freedom of expression of their users by seeking to avoid or minimize the impact of government restrictions on freedom of expression;
- respect and work to protect the privacy rights of users when confronted with government demands, laws or regulations that compromise privacy in a manner inconsistent with internationally recognized laws and standards;
- identify circumstances where freedom of expression and privacy may be jeopardized or advanced and integrate these Principles into their decision making in these circumstances;
- prioritize the safety of personnel over these principles.

To apply these principles, Orange ensures that for each major event resulting from a government request, the request is justified in accordance with local law. (it comes from a state department with authority to make this request) and international laws. Orange also issues a decision on the proportional nature of the request.

To ensure traceability of this approach, Orange has implemented a procedure for responding to these major events; it involves receiving a formal, traceable request, i.e. an order written

and signed by a public authority with the necessary jurisdiction and based on a law or regulation.

If the request is not made in compliance with these formalities, Orange reserves the right to alert the international community and supranational authorities.

5.4. The indicators presented in this report

To report on action taken by governments regarding freedom of expression and protection of privacy, Orange has chosen two indicators:

- government requests for interceptions,
- government requests for customer data.

To facilitate comparison between the many reports by the industries in question, Orange has decided to use the most commonly used indicators.

The 'interceptions' and 'customer data' indicators refer to the number of government requests made to Orange. A single request may cover multiple customers, and a single customer may be involved in several successive requests over the course of the year.

Requests can differ depending on the issuing authorities and countries. In order for Orange to carry out these requests, they must meet three formal requirements:

- the authority making the request must have jurisdiction to do so,
- the request must be made via formal channels,
- the request must comply with the country's laws and regulations.

Once all of these elements have been verified, the request is either implemented, rejected, or referred back to the requesting party to obtain the missing information needed to assess the request.

5.4.1. Interception of communications

This indicator represents the number of requests made by governments or other public authorities, including requisition orders and administrative requests requiring the disclosure of the content of calls.

The ETSI (European Telecommunication Standardization Institute) has set out an international standard defining interception as "legally sanctioned official access to private communications."

This standard specifies that:

- Information on how interception measures are implemented in a given telecommunications installation must not be disclosed to unauthorized persons;
- Information on the techniques used to target the identities and services that are the subjects of the interception must not be disclosed to unauthorized persons;
- Only the overall figure is published, except if a managerial decision or national legislation prevents this. A managerial decision may be made based on the fourth GNI principle, which has been adopted by Orange: protecting our staff under all circumstances. The decision can be made by the CEO of the subsidiary or by the Group's executive management.

The table below does not show any figures for some countries. In some cases, this is due to local legal constraints, while in other cases the authorities may have direct access to the content of communications, meaning that no request was made to Orange, even though the interceptions might have taken place.

5.4.2. Seizure of customer data

This indicator corresponds to the total number of requests made by different players, including the government, the judicial system, or the police, requesting data including:

- Call details (traffic data such as originator, recipient, frequency, duration, etc.)
- Customer identification data (first and last names, address, date of birth, etc.)
- Geolocation (relays or GPS coordinates)
- Billing and payment data

This indicator also covers all types of communications made using landlines, broadband and mobile lines, regardless of the type of device used (landline handset, mobile phone, smartphone, TV, PC, tablet, or smart device) or the Orange package involved.

Interception and customer data requests - 2020

Country	Number of employees	Number of customers	Interceptions[10]	Customer data
France[1]	80,948	66,503,372	12,891	66,714
Poland[2]	11,397	20,672,917	not published	not published
Spain	7,698	20,736,930	50,066	56,775
Belgium[3]	1,723	5,124,485	327,662	
Romania	3,652	10,185,484	not published	156,000
Slovakia	1,180	2,801,559	Unavailable	12,392
Moldova	1,342	2,065,518	Unavailable	6,432
Morocco	1,296	13,749,583	not published	not published
Senegal	1,869	11,072,275	38787	
Mali	743	12,368,595	0	10,950
Côte d'Ivoire	1,578	14,910,597	0	9,457
Egypt	3,581	27899581	not published	not published
Jordan	1,701	2779445	0	12,300
Madagascar	680	2366096	6528	Unavailable
Botswana	302	1419477	Unavailable	Unavailable
Cameroon	627	9267672	0	16,269
Guinea Conakry	408	8507360	Unavailable	Unavailable
Congo	1,445	10514697	9	1,154
Tunisia[4]	1,200	4500000	10,140	7,264

Not published: the local authorities restrict publication of this information
Unavailable: Orange did not collect the data
0: Orange did not carry out any interceptions

1 For France, the data presented refers only to requests made by the intelligence services, and is taken from the annual report of the National Commission for the Control of Intelligence Techniques (CNCTR). It covers the data from all carriers in France. Requests are presented gross of any refusals.
2 This data was published by the Polish authorities in an official report until 2015. Reports for subsequent years have yet to be published.
[3] The regulations in force require Orange to publish the 2 indicators together
4 As Orange Tunisia is not fully consolidated, the numbers of customers and of employees in Tunisia are not included in the consolidated figures published by the Group.

5.5. Major events related to freedom of expression

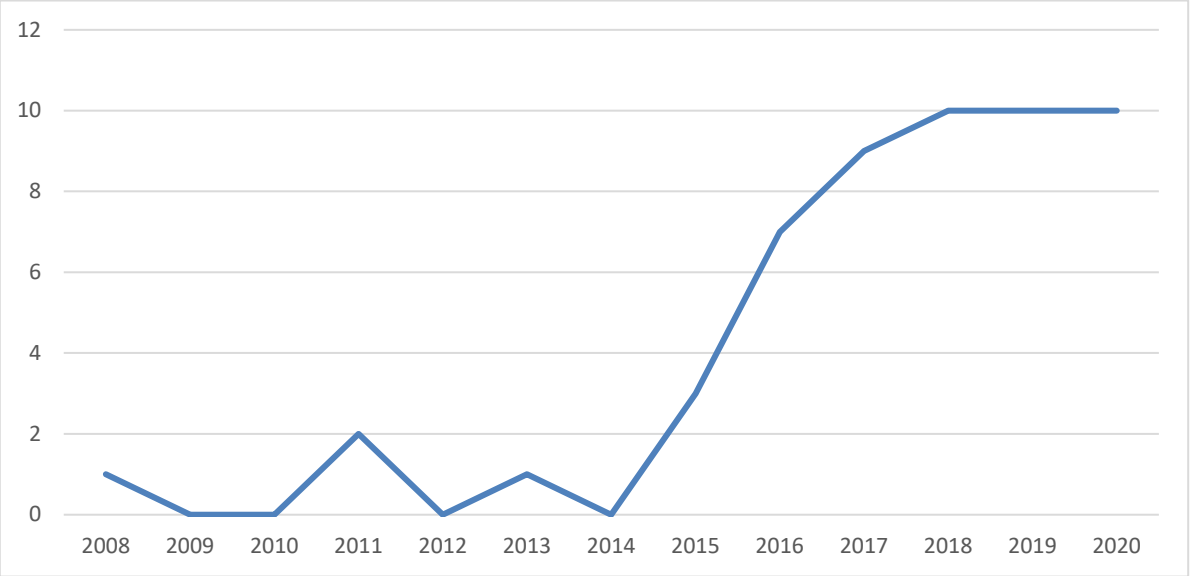
For a telecommunications carrier, major events are occasional government requests that affect a large number of customers at the same time. These events can include

- network shutdowns resulting in the outage of all services requiring internet or SMS access, or voice services;
- shutdowns of certain targeted services, e.g. cutting off access to social media; or
- the mass sending of government information by SMS, for example, and
- requests for information on all Orange customers.

In 2020, the Group reported 10 major events of this type, which is the most seen since 2008.

The growing number of requests in 2019 is primarily due to multiple requests for shutdowns made by certain governments in their countries. The same applies in 2020.
In 2019 and 2020, we received a large number of requests during the periods before and after elections, and several requests may have been made by the same country.

Number of requests for shutdowns 2008 - 2020



Major events make it impossible to publish details of these requests, such as the countries involved, dates, circumstances and reasons given. Publishing this information could expose our staff to risks in the various Group countries.
This position is enshrined in principle 4 of the GNI, which recommends protecting the safety and freedom of all staff who may be endangered.

5.6. Content restriction requests

Orange's position in terms of content restriction is to obey the laws in force in the countries in which we operate. Orange obeys administrative and legal requests to remove illegal content. We act on government requests regarding specific cases. In most cases, the content restriction applied involves blocking a website or an IP address. As a telecommunications carrier, Orange does not examine internet content and cannot block specific content, only domains.